REMARKS

Claims 1-12 and 14-26 are pending in the application. Applicant reserves the right to pursue the original claims and other claims in this and other applications.

Claims 1-7 stand rejected under 35 U.S.C. § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. The Office states that that the term "accessing said encryption key on said network communication device during an encrypted communication" is unclear how the "encryption key (the encryption key before the replacement) is accessed during an encrypted communication." Applicant respectfully traverses the rejection.

Although Applicant respectfully suggests that the claim meaning clear when viewed *in toto* in that the "encryption key" in the last clause of claim 1 referred to "said new encryption key" and did not refer to "said existing encryption key," claim 1 has been amended for additional clarity.

Claims 1, 6-8, 14-20 and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Serceki et al. (U.S. Pat. Pub. No. 20030078072)("Serceki") in view Linkola et al (U.S. Pat. No. 2003/0078072)("Linkola"). This rejection is respectfully traversed.

Claim 1 recites:

> A method of updating and using an encryption key used by a wireless station for encrypted communications with a wired portion of the network, said method comprising:
>
> physically separating from said wireless station a network communications device;
>
> physically connecting said separated network communications device to an encryption key updating device which is connected to a wired portion of said network said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device;

replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network;

physically reconnecting said network communications device containing said new encryption key with said wireless station of said network; and

accessing said new encryption key on said network communications device during an encrypted communication."

Serceki discloses a "method for providing configuration information for use in installing a new wireless station to a wireless network that minimizes errors..." According to Serceki, the "configuration information is distributed by storing the configuration information onto a device with a memory and then distributing the device to the users interested in installing new wireless stations. The device is attached to a computer to which the wireless station is coupled, initiating a transfer of the configuration information. The computer uses the configuration information to configure the wireless station. The method also provides a way to limit access to the configuration information through the use of encryption and limiting the number of times the configuration information is retrieved. The method is also an effective way to distribute security keys for encryption systems whose purpose is to secure communications in a wireless network." (Serceki, Abstract)

As articulated in the Office Action dated October 6, 2006, Serceki fails to disclose at least "accessing said encryption key on said network communication device during an encrypted communication." (emphasis added). The invention of Serceki is essentially a method of transferring information between two computers systems that are not physically connected by using a storage device as a conduit between the two systems, e.g., a "wireless station" and a "wired portion of a network." Thus, in the invention of Serceki, a storage device is used to transfer data, e.g., configuration information or security keys, between the two systems.

Linkola is cited by the Office as disclosing "accessing encryption key on said network device during an encrypted communication." Applicant respectfully disagrees.

Applicant notes that the Office has not specifically identified the relevant element or part of Linkola. Thus, Applicant has difficultly in properly responding to the Office Action. Nevertheless, in an effort at a complete response to the Office Action, for the purposes of this Amendment, Applicant presumes that the Office is referring to the subscriber identity module (SIM) of Linkola. If the Office is referring to an element other than the SIM as disclosing an "encryption key on said network device during an encrypted communication," then the Applicant respectfully requests that the Office withdraw the previous Office Action and reissue a new Office Action identifying with specificity the relevant element(s) of Linkola and the pertinence of such parts.

Linkola discloses a mobile phone system for telecommunications that includes a SIM chip. The SIM chip contains and provides/identifies to a communications system an international mobile station identity (IMSI) code. An IMSI is a phone number, not a security code used during encrypted communications.

Linkola fails to disclose at least "accessing said encryption key on said network device during an encrypted communication." Although Linkola provides a mobile phone having a SIM having a IMSI that can be updated to a new IMSI, thus, giving a mobile phone a new phone number, the SIM of Linkola does not provide for "accessing said encryption key on said network device during an encrypted communication." Linkola's SIM is not disclosed as including encryption information. Thus, Linkola fails to disclose an "encryption key on said network device" and as such, Linkola fails to disclose any element that makes reference to an "encryption key on said network device," including the element "accessing said encryption key on said network device during an encrypted communication." Thus, the combination of Serceki and Linkola do not disclose the claimed invention. As such, the rejection of claim 1 should be withdrawn and the claim allowed.

Thus, if the teachings of Serceki and Linkola were combinable, which they are not, the varied teachings of Serceki and Linkola could not be combined to achieve the claimed invention.

Moreover, the teachings of Serceki and Linkola are not properly combinable. Serceki teaches distributing encryption information through the use of a storage device from a first system and to a second system, where the information is transferred from the storage device to the second system The storage device is removed from the second system and the transferred information is accessed by the second system as part of said second system without the need for accessing the storage device. Linkola teaches creating and updating information on a SIM card, but does not teach using the SIM card to transfer information from one system to another system. Furthermore, the information on the SIM card does not contain encrypted information. Thus, the teachings of Serceki and Linkola are not combinable.

Claims 6-7 depend from claim 1 and are allowable for at least the reasons noted above with respect to claim 1.

Claims 8, 14-20, and 26 have similar limitations as claim 1 and are allowable for at least the reasons noted above with respect to claim 1. Accordingly the rejection of those claims should be withdrawn and the claims allowed over Serceki and/or Linkola.

Claims 2-3, 9-10, and 21-23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Serceki in view of Linkola and in view of Campbell, Jr. (U.S. Pat. No. 4,369,332)("Campbell"). This rejection is respectfully traversed.

Claims 2-3, 9-10, and 21-23 have similar limitations as claim 1 and are allowable over the combination of Serceki and Linkola for at least the reasons noted above with respect to claim 1.

Campbell discloses at least an "apparatus and method for generating a unique working key variable for controlling the operation of an encryption/decryption device during each user specified time period. The apparatus generates each working key variable by encrypting a user specified value, unique for each specified time period, under control of a fixed key variable stored in the apparatus. After the user specified value has been encrypted, the apparatus utilizes the encrypted (working) key variable to control the encryption/decryption of data during the corresponding user specified time period." (Campbell, Abstract)

Campbell fails to disclose "accessing said encryption key on said network communications device during an encrypted communication." As such, Campbell fails to cure the deficiencies of Serceki and Linkola. Therefore the rejection of these claims should be withdrawn and the claims allowed.

Claims 4-5, 11-12 and 24-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Serceki in view of Linkola and in view Trieger (U.S. Pat. No. 6,226,750)("Trieger"). This rejection is respectfully traversed.

Claims 4-5, 11-12 and 24-25 have similar limitations as claim 1 and are allowable over the combination of Serceki and Linkola for at least the reasons noted above with respect to claim 1.

Trieger disclose a "method and system for tracking communications in a client-server environment. The method includes the steps of sending a first request from the client to the server over a first connection, sending a first key from the server to the client over the first connection, sending the first key from the client and a second request to the server over a second connection, and sending a response to the second request and a second key distinct from the first key from the server to the client over the second connection. The system includes a client for establishing a terminal connection with a server and a server in communication with the client. The server further includes key generator means generating a plurality of keys for transmission to the client, authentication means in communication with the key generator means receiving the keys from the client to recognize the keys at the server, and discarding means linked to the key generator means for disposing of previously transmitted keys." (Trieger, Abstract)

Like Serceki and Linkola, Trieger also fails to disclose at least "accessing said encryption key on said network communications device during an encrypted communication." As such, Trieger fails to cure the deficiencies of Serceki and Linkola. Therefore, the rejection of these claims should be withdrawn and the claims allowed.

In view of the above, Applicant believes the pending application is in condition for allowance.

Dated: October 17, 2007

Respectfully submitted,

By _____

Thomas J. D'Amico
Registration No.: 28,371
Michael A. Weinstein
Registration No.: 53,754
DICKSTEIN SHAPIRO LLP
1825 Eye Street, NW
Washington, DC 20006-5403
(202) 420-2200
Attorneys for Applicant